WHAT IS CLAIMED IS:

1. A high-performance Booth-encoded Montgomery module for performing the computation of $A * B * r^{-1} \pmod{N}$, where A, B and N are the (n-bit) multiplicator, (n-bit) multiplicand, and (n-bit) modular number, respectively, and $r = 2^n$, the module comprising:

a Booth encoder for receiving two bits of A to perform a Booth encoding process, so as to produce a Booth code for output;

a multiplicand selector for receiving B and the Booth code output from the Booth encoder so as to select a multiplicand based on the Booth code for output;

a first carry propagate adder for adding the output of the multiplicand selector and a previous computation result to output;

a multiplexer for receiving four inputs 0, N, 2N, and 3N from a lookup table and selecting one of the inputs to output;

a second carry propagate adder for adding the outputs of the first carry propagate adder and the multiplexer to output; and

a shifter for shifting the output from the second carry propagate adder to right by two bits, so as to produce a computation result.

2. The high-performance Booth-encoded Montgomery module as claimed in claim 1, further comprising a register for buffering the computation result.

3. The high-performance Booth-encoded Montgomery module as claimed in claim 1, wherein the multiplicand selected by the multiplicand selector is 2B, B, 0, -B, or -2B.

4. The high-performance Booth-encoded Montgomery module as

claimed in claim 3, wherein the Booth code is 3-bit.

5. The high-performance Booth-encoded Montgomery module as claimed in claim 3, wherein the input 2N is produced by shifting the input N to left with a shifter so that only three inputs 0, N and 3N are required in the lookup table.

6. The high-performance Booth-encoded Montgomery module as claimed in claim 1, further comprising a modular selector for selecting 0, N, 2N, or 3N to be added to the second carry propagate adder.

7. The high-performance Booth-encoded Montgomery module as claimed in claim 1, wherein each carry propagate adder has a row of full adders, and every four full adders are grouped together, such that two corresponding full adder groups of the first and second carry propagate adders form a Montgomery cell for being used as a pipelining stage.

8. The high-performance Booth-encoded Montgomery module as claimed in claim 7, which has a plurality of Montgomery cells for constructing a Montgomery modular multiplier.

9. The high-performance Booth-encoded Montgomery module as claimed in claim 8, further comprising a multiplexer and a data loop to reuse the Montgomery cells, so that the cell number can be reduced by 1/2.